REMARKS

This application has been carefully studied and amended in view of the Office Action dated March 28, 2006. Reconsideration of that action is requested in view of the following.

The claims and in particular, independent claims 1 and 3 have been carefully reviewed in view of the rejection of the claims under 35 U.S.C. 112. At the outset applicants wish to thank Examiner Ho for the detailed analysis of the terms in question in the independent claims including the likely meaning of the terms being questioned. With regard to the meaning of "irreversible linking" the actual meaning is what was indicated in paragraph 3 of the Office Action as the second meaning, namely, a specialized cryptographic process such as a hash encryption. Support for this meaning is found in Figure 1 and in particular in the description relating to that figure. See, for example, the second paragraph on page 5 in combination with the last three paragraphs on page 4 relating to a hash machine active in the method and system according to the invention. Independent claims 1 and 3 have been amended to now refer to the irreversible linking as "by hash encryption". As regards the additional features of claim 1 referred to in the Section 112 rejection, with respect to the security module generating a secret which remains unknown to a document producer and with respect to it not being possible to draw conclusions about the secret, it is observed that Examiner Ho has pointed out that the known procedures do not allow generating a secret which remains unknown to a document producer and whereby it is not possible to draw conclusions about the secret. The solution described in this application regarding the present invention is specifically described in process step 1 at page 11 which relates to Figure 2. This implementation implements the usage of a random number that is encrypted together with an identification number of the security module. The encryption is performed with the public key of the authentication unit so that the document producer can not

gain access to this temporary secret and it can only be encrypted by the authentication unit. Claim 1 has been amended to state that the document producer can not gain access to the secret which can only be encrypted by an authentication unit.

Reconsideration is respectfully requested of the rejection of claims 1-4 as anticipated by Houser. The present invention relates to a security module for producing forgery-proof documents by a hash value which is output from the outlet valve. The invention is directed to implementations which are contrary to what is described in Houser.

Houser relates to an electronic document verification system and a corresponding method. The nature of the embedded object 130 according to Houser and the embedded security object according to the present invention is important. The technical teaching of Houser is that electronic documents are received (150) and verified and afterwards embedded (130 (with reference to Fig. 1)), whereas the present invention implies a secret which remains unknown to a document producer.

According to the technical teaching of, for example, claim 1 this unknown secret together with information that reveals details about the identity of the security module, is transferred in encrypted form to an authentication unit. The combination of the secret and the information that reveals details about the identity of the security module according to the invention allows securing authenticity with significantly less information bits necessary.

For example the security module according to the invention allows producing indicia which are significantly smaller that known indicia.

Examiner Ho's attention is directed to the fact that digital signatures according to the state of the art (Houser) require a huge amount of data to be transferred.

This is especially disadvantageous if the size of the data is of importance. A very important field for generating smaller forgery-proof documents is the generation of digital postmarks. The United States Postal Services have introduced an information based indicia program IBIP. This program generates digital franking marks with a suitable size.

To demonstrate the difference between this information and shorter information secured according to the present invention, attached are copies of letters with a digital franking mark produced with a security module according to the present invention.

In order to achieve this advantage of the invention, the security module according to claim 1 contains the characteristic that the output value of the combination machine (K2) is used to form an irreversible hash value and the hash value is output from the outlet valve (2).

These characteristics are not found in Houser which proposes a usage of digital signature algorithms for securing data. In contrast, the present invention relates to a security module for producing forgery-proof documents by a hash value which is output from the outlet valve and which involve implementations contrary to Houser.

In view of the above remarks and amendments this application should be passed to issue.

Respectfully submitted,

By Harold Pezzner

Harold Pezzner
Registration No.: 22,112
CONNOLLY BOVE LODGE & HUTZ LLP
1007 North Orange Street
P.O. Box 2207
Wilmington, Delaware 19899
(302) 658-9141
(302) 658-5614 (Fax)
Attorney for Applicant